00126287/9
DIALOG(R)File 256:TecInfoSource

00126287 DOCUMENT TYPE: Review

PRODUCT NAMES: PayPal (781924)

TITLE: Alternate Online Payment Finds A PayPal
AUTHOR: Cleary, Mike
SOURCE: Interactive Week, v7 n31 p40(1) Aug 7, 2000
ISSN: 1078-7259
HOMEPAGE: http://www.interactive-week.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

With e-commerce companies sticking to credit-card payments primarily, alternative payment systems still lack attractiveness. However, One company, PayPal.com, uses the Internet's most popular application (e-mail) and one of bricks-and-mortar retailers' favored payment methods (credit cards) to allow merchants and shoppers to conveniently transfer money over the Web. Analysts like PayPal.com's potential, saying that the ability to handle electronic consumer transactions is paramount to success; but, alternative payment systems, such as Beenz or Flooz, as well as Internet service provider (ISP)-based micropayment systems, have only gotten the tiniest market share. PayPal.com charges merchants 1.9 percent of the transaction's cost (in contrast to up to 3.5 percent charged by credit card companies). PayPal.com can charge less because credit-card companies do not process the transactions. PayPal.com, which was acquired by X.com, creates accounts for all merchant and individual customers. Each member deposits money into PayPal.com's system through credit-card or bank accounts. Merchant members say they like the convenience of PayPal.com, but consumers may not be too enthusiastic, since they are not offered protection against fraud occurring over the Internet.

COMPANY NAME: PayPal Inc (671908)
DESCRIPTORS: Credit Cards; E-Commerce; E-Payment
REVISION DATE: 20030130
?

0206096

Debit cards: Payroll Card Ups Fees

American Banker - October 6, 1997; Pg. 18; Vol. 162, No. 192
SECTION HEADING: Future Banker
ARTICLE TYPE: Feature Article
DOCUMENT TYPE: Journal LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 415

TEXT:

NTS, Inc., a business unit of First Data Corp. that serves the trucking industry, has developed a new payroll debit card that banks can use to attract commercial customers and increase fee income. Called TransPay, the technology allows

company payrolls to be transferred to employee cardholders who then can access their money at nearby ATMs. Access to ATMs is currently made possible through a relationship with CoreStates National Bank, of Philadelphia, which has its name stamped on the front of the cards. Six major banks have shown interest in adding TransPay service to their commercial business platforms, says NTS business development director Mike Brunner, though he would not name the institutions.

Every time the card is used, the bank sponsoring the card collects a fee. The system is currently set up so that the employer pays for the first transaction fee, loading the paycheck onto the card. Employees pay a $2 or $3 fee per subsequent transaction.

When an employee receives a payroll or expense reimbursement electronically through TransPay, the employee can withdraw the funds at an ATM, generate personal checks through Western Union or transfer money into a savings or checking account. The card is accepted at ATMs in the MAC, Honor and Plus networks.

TransPay works best for companies with many remote employees and traveling sales forces, such as Dallas-based Claim Services Resource Group (CSRG), a temporary medical and dental staffing agency and the first national firm to distribute the cards. CSRG employs as many as 2,000 people over the course of a year, many of whom have heavy travel schedules. CSRG's chief financial officer Phyllis Farragut says that TransPay has cut payroll time by 75 percent because the accounting department can simply go to the computer to make employee money available. Says Brunner, "Businesses that will benefit most are those that produce a central payroll and have many remote locations with employees scattered around the nation, (where the company) must deliver overnight express paychecks. TransPay eliminates couriers, cuts labor and distribution costs, and reduces fraud. Security is maintained by a multi-level password system."

The card is also an indirect way for banks to service unbanked workers, winning business away from check cashers. "(One) target market is unbanked employees, those 20 percent of the population who can't get a bank account for any reason," says Brunner. But the card also compliments the banking system. "An employee can transfer funds from the card to up to three bank accounts," he says.

-peterson<at>tfn.com

08197310 Supplier Number: 68866240 (THIS IS THE FULLTEXT)

Banks out in the cold?

Cards International, p14
Dec 13, 2000
ISSN: 0956-5558
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 1599

TEXT:

The world's leading financial institutions will have to move quickly if they are to counter the threat from new `virtual' payments services that can bypass the banking system altogether. CI investigates

FINANCIAL INSTITUTIONS could lose up to $100 billion in future payments revenues by 2008 if they fail to face up to the threat presented by online payments providers and telcos, according to research from the Boston Consulting Group (BCG).

The figure accounts for nearly a third of the estimated $310 billion of total payments revenues by 2008, representing a huge dent in the financial sector's market share.

While banks have traditionally used their unique access to clearing and settlement systems to build up comprehensive customer databases and cross-sell a range of financial products, BCG states that the open standards of the Internet are fundamentally reshaping how businesses and consumers transact. BCG forecasts that B2C e-commerce could reach $200 billion in the US alone by 2004, versus $60 billion this year. In addition, the online B2B sector is forecast to grow to $5 trillion in the US by 2004, representing as much as 40 percent of overall B2B e-commerce.

The report asserts that the Internet has created new opportunities for an array of new players to facilitate transactions online. Some, like ProPay or PayPal, allow customers to make person-to-person payments at online auctions, while telcos are well placed to develop payment services both offline and online.

"The payments landscape is increasingly crowded and complicated, with overlapping and competing solutions covering each part of the value chain and each type of payment; person-to-person, customer-to-business, business-to-customer, business-to-business. At one time banks were masters of this entire space; now they have only settlement, the least attractive part of the value chain, to themselves - and even there, others are encroaching," BCG notes.

While stressing that the future payments landscape is open to question, BCG outlines a number of potential outcomes.

One possibility is that banks will fait to react rapidly to the threat presented by new payment services providers in the virtual world. These providers are not only offering low-cost alternatives for payments in the micropayments and person-to-person segment, but are also looking to gain market share in C2B, B2C and even B2B payments through attractive customer-centric service propositions right across the payments value chain.

This proliferation of new online providers will push down prices and lead to a loss in revenues and market share for the banks.

"(Online providers can) offer merchants low-cost, secure alternatives to today's card-based systems. These trends should increase online payments volumes, but, if online providers capture significant share, they would bring much lower unit prices, meaning overall revenues would fall," the report says.

While BCG accepts that early Internet payments systems have largely failed, new providers, such as PayPal Billpoint and ProPay, offer more compelling business models in a market that now has enough critical mass for payments providers to generate credible revenues from merchant fees, float interest and currency spread. PayPal, for example, has attracted over 3 million accounts in less than 12 months through focusing on cost-effective low-value payments, initially on Internet auction sites. The service is free for P2P customers, leading the company closer to achieving critical mass, BCG said. The company is also moving into the B2B and B2C markets, and has recently expanded to Europe through a partnership with ING (see page 6).

Should banks fail to address this issue, they stand to lose up to $50 billion in payments revenue - 60 percent of the online market - to online payments providers by 2008, as online cheque and cards payments migrate to new providers, previously offline payments are moved online, and extra transactions are generated by the new payments mechanism.

However, BCG believes banks could become powerful players in this area if they fight back by providing product offerings and pricing to counter the competitive threat. Nick Viner, vice president of Boston Consulting Group, believes banks must stay in the payments business to defend their overall business. "Transactions represent the defining relationship with your primary financial account," he said.

Viner also believes that banks still have great opportunities to develop new profits from their payments franchises, albeit facing intense competition from both online providers and telcos.

Banks could extend their existing account infrastructure onto the Internet -although this would ultimately require them to cannibalise their existing business, driving down not only revenues, but also costs.

Financial institutions also could leverage their existing customer relations to halt or reverse their falling market share, and provide online trust and security services for Internet transactions.

Viner identified Wells Fargo, Chase and Citi as financial institutions that had seized the e-commerce agenda, with European banks, such as those based in The Netherlands, likely to prove winners. He pointed to Deutsche Bank as an institution investing heavily in this area.

"Banks with scale like Citi or Wells Fargo can to go head-to-head with the new entrants and surpass them if possible. Smatter institutions ... need to find ways to protect their (customer) position," said Viner.

Telcos, ranging from device manufacturers to network providers, are also in a strong position to capture key segments of the payments value chain from origination (e-wallets) to authentication (digital certificates) to settlement (aggregation).

Mobile telephones with embedded chips make ideal payments wallets for both physical and virtual payments, and consumers are increasingly viewing access devices as a means to conduct commerce as well as communicate.

In addition, mobile devices have a built-in capacity to read the digital certificate on an embedded chip and encrypt a transaction, either across the mobile network or through Bluetooth. This means the mobile device is effectively invisible to the consumer, an essential component in any payments proposition.

The mobile telephone could potentially act as a "portable hand-held wallet", and could offer a range of functionality, including e-purse, credit and debit purchases and even loyalty programmes. Prepaid mobile telephones would make a powerful vehicle to make payments by those not able to obtain a credit card or bank account.

More importantly, BCG states that the telcos can exploit their key assets - a large customer base and extensive customer information - to sell payments services. Following competition within the telecommunications industry, telcos will need to find alternative sources of revenue, the

consultants continue.

BCG believes that telcos could eat into retail domestic card and cheque payments and charge lower fees to merchants, meaning average revenues per payment could fall from a `cost base' of $0.82 to $0.57, with telcos picking up $47 billion in physical and online revenues from the banks.

Viner identified Australia's Telstra, the UK's BT, Spain's Telefonica, Deutsche Telecom and Finnish handset manufacturer Nokia as good examples of telcos that could make a major splash in the payments pool.

BCG believes, however, that banks could remain the core payments providers by using their influence and forging alliances to develop opportunities on the Internet, thus ensuring they maintain their core position in the payments business.

Areas of strength include financial institutions' core customer franchises and their role as trusted intermediaries - with BCG citing Identrus as a good example of a bank effort in the e-commerce world. Banks also could provide a major role in defining standards and have the capital to buy savvy new technology and technology providers.

BCG contends that new EMV smart cards, chip cards used for Identrus and other bank certification schemes should boost the secure image of banks as trusted intermediaries for payments on the Internet.

Given such an outcome, banks would be able to defend their franchise against the dual threat of online providers and telcos and maintain revenues, but merchant fee income would be likely to fall. BCG estimates that revenues per payment would fall to $0.64 and banks would earn $288 billion in 2008.

Banks, however, could also exploit current developments to generate new revenues - especially in the B2B space.

Banks have an opportunity to develop trust services on the Internet, which can ensure that the much-hyped B2B e-commerce mushrooming would take place, although there is also a risk that e-marketplaces could fulfil many of the value-added services themselves.

According to BCG, online B2B payments revenues could be worth $20 billion by 2008, while the associated revenues banks earn from providing value-added services in the B2B market-place - such as letters of credit, invoice management and certification financing - could amount to $30 billion. However, to generate such additional revenues, banks need to work together soon to develop common standards with widespread credibility.

SOME CURRENT PLAYERS IN THE ONLINE CONSUMER PAYMENTS MARKET

beenz	Virtual currency, earned by visiting sites, registering with merchants or making purchases. Can be spent at merchants, or used to pay credit card bills. Available over browsers, mobiles, PDAs, IDTV, smart cards.
Billpoint	Official payment mechanism of eBay, jointly owned by eBay and Wells Fargo. Allows buyers to pay for auction items using credit card or electronic cheque, with funds paid directly to seller's account. Provides electronic wallet option for frequent users.
eCatalystOne	Prepaid cash card bought at retailers, and activated by PIN entry at merchant sites. Allows consumers to make anonymous purchases. Pilot launched in Q3 2000.
eCharge	Aggregator, charging payments against telephone bills, ISP bills, credit cards, or prepaid deposits. Provides security through download of

	digital certificate to user's PC. Allows `sub-accounts' for employees or children.
eMoneyMail	E-mail payment interface for transferring money between credit cards and/or bank account of senders and recipients. $1 flat fee for senders. Site powered by Bank One.
iPin	Aggregator charging payments to telephone or ISP bill, credit card, or bank account. Customers use PIN to make payments. Software download required before system can be used.
PayPal (X.com)	Stored value system of prepaid customer accounts Allows e-mail payments between consumers across all access devices. Provides value-added services including mass payments, and provides a transaction log compatible with Intuit and Microsoft products.
ProPay	Stored value system of prepaid customer accounts. Allows customers to transfer money between accounts, or to withdraw money via their bank accounts.
QPass	Aggregator, billing transactions to credit card on a monthly basis. Primary focus on merchants selling digital content. Provides optional `Power Wallet' digital wallet. Investors include American Express and Andersen Consulting.

Source: Boston Consulting Group

PUBLISHER NAME: Lafferty Publications Ltd.
COMPANY NAMES: *Boston Consulting Group
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *7392000 (Business & Mgmt Consulting)
INDUSTRY NAMES: BANK (Banking, Finance and Accounting); BUSN (Any type of business); INTL (Business, International)
SIC CODES: 8742 (Management consulting services)
NAICS CODES: 54161 (Management Consulting Services)
SPECIAL FEATURES: LOB; COMPANY
?

02367381 117541709

Identifying effectiveness criteria for Internet payment systems

Shon, Tae-Hwan; Swatman, Paula M C

Internet Research v8n3 PP: 202-218 1998 CODEN: IRESEF ISSN: 1066-2243
JRNL CODE: NTRS
DOC TYPE: Periodical; Feature LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 9810

DESCRIPTORS: Internet; Electronic data interchange; Computer networks; Payment systems; Studies
CLASSIFICATION CODES: 5220 (CN=Information technology management); 9130 (CN=Experimental/Theoretical)
PRINT MEDIA ID: 46159

ABSTRACT: The Internet, since its commercialisation, has expanded with tremendous rapidity. This development has been still further assisted by the creation of the World Wide Web, which has caught the imagination of users around the world. As the marketing and provision of goods and services over the Web continues to grow, the missing factor appears to be a well-accepted and well-trusted method of paying for these products and services. This paper discusses the problem of Internet payment systems (IPS) and reports the results of a research project which attempts to identify and classify effectiveness criteria for IPS. The project was undertaken by means of a Delphi survey of experts in IPS usage and classified types of IPS providers, as well as the factors which each group considers most important. This information was used in the development of our set of IPS effectiveness criteria.

TEXT: Tae-Hwan Shon: Tae-Hwan Shon and Paula M.C. Swatman are at the Department of Information Systems, Monash University, Caulfield East, Victoria, Australia. E-mails: tshon@ponderosa.is.monash.edu.au paula.swatman@is.monash.edu.au

Paula M.C. Swatman: Paula M.C. Swatman are at the Department of Information Systems, Monash University, Caulfield East, Victoria, Australia. E-mails: tshon@ponderosa.is.monash.edu.au paula.swatman@is.monash.edu.au

Introduction

The Internet, connecting more than 140 countries around the world, is known to most people as the global "network of networks". According to Network Wizards (1996) the number of host computers on the Internet increased from 992,000 in July 1992 to 12,880,000 in July 1996; and more than 488,000 domains and 134,365 networks were found on the Internet in July 1996. Internet facilities allow users to send electronic mail (e-mail) to one another, download useful files and connect one host computer to another. These abilities, while impressive, are merely an example of what the Internet can offer to its users around the world. Krol (1994) suggests that the most important aspect of the Internet is its ability to allow everyone to access the network. The World Wide Web (WWW, or "the Web") was developed at CERN, the European Laboratory for Particle Physics in the early 1990s. Eager and Pike (1995) describe the Web as:

- An Internet-based navigational system.

- An information distribution and management system.

- A dynamic format for mass and management systems.

The Web's design is based on the HyperText Transport Protocol (HTTP), which allows users to create hyper-media-based documents[1] called "Web pages" using the HyperText Markup Language (HTML). An important feature of a Web page is that it can easily be linked to any other Web page on the Internet. A "Web browser" - a term used only on the Web - is the most popular program on the Internet today. This is a public-access client program which enables users to navigate and access any Web page (Krol, 1994). The most important aspect of the Web is its ability to support multimedia applications such as graphics, sound, movies or interaction between users. Cronin (1996) points out that the development of the Web (and its associated applications, such as Web browsers and "search engines") has made the Internet much easier to use and navigate and has greatly increased the Internet's attraction for and use by individuals and organisations.

The Internet was originally used by individual academics, universities and government agencies (particularly in the military) for research and development purposes. Since the commercialisation of the Internet in 1993, this group has been joined by companies of all sizes, wishing to advertise and trade goods and services both locally and globally (Kalakota and Whinston, 1996). According to Yahoo (1996), there were more than 23,000 companies on the Web as of October 1995. A survey conducted by Gray (1996) indicates that more than one million Web sites were found as at 1 January 1996. Commercial activities already absorb more than 50 percent of the Internet's usage and this proportion is increasing daily.

Yet, despite this enthusiasm and rapid growth, the Internet has been recognised as a difficult place to do serious business (see, for example, Poon and Swatman 1995, 1996, 1997). Most companies limit their business activities to creating on-line catalogues, advertising products and communicating with customers through e-mail, although it is not difficult to imagine the potential of the Internet as a true market medium. Impediments to maximum use of the Internet for commercial use include the lack of a standard interface and fears concerning the privacy and security of personal information. A major problem, however, is the lack of an integrated financial transaction system suitable for an open electronic marketplace such as the Internet. How the consumer will pay for goods and services and how the provider will receive the payment securely over the Internet are issues which are being seen as some of the most important success factors for Internet commerce.

To overcome these problems, many individuals and organisations have been developing financial transaction systems for the Internet which are becoming known as Internet payment systems (IPS). Clearly, there is considerable interest in the concept of IPS (more than 30 IPS proposals have been published on the Web since the middle of 1996). Each of these has some features which are unique, although there are also a number of similarities. Most current IPS already guarantee security of transactions by applying various technologies to the transmission of the financial message (some of them can even protect the customer's privacy. However, are security and privacy the only issues which need to be resolved when considering an IPS? How efficient are currently-available IPS? Are there any other factors which must be considered for an IPS to be really effective? Which entities are involved with the use of an IPS?

This paper attempts to answer some of these crucial questions, by focusing on two specific aspects of an IPS:

- (1) the identification of the major entities involved with IPS; and

- (2) the development of effectiveness criteria for IPS.

Initially, this paper briefly describes the different types of IPS and their known advantages and disadvantages. Next, we describe the methodology of the research project and discuss the project itself; both the Delphi survey, by means of which we obtained expert input into the development of our effectiveness factors for IPS; and the way in which the factors evolved. The paper concludes with a discussion of future research approaches which could further extend this work.

Internet payment systems

An exact definition of an IPS is difficult to find (and varies widely from one organisation to another). Partly, this difficulty is due to the "newness" of the IPS concept and the rapid rate of development of the concept; but it is also due to the fact that the term IPS can mean different things to different people. For the purposes of this paper, therefore, we define an IPS as:"

Any conventional or new payment system which enables financial transactions to be made securely from one organisation or individual to another over the Internet."

By its definition, IPS is clearly a sub-type of the wider group known as electronic payment systems (EPS). An EPS can be broadly defined as "any transfer of funds initiated through an electronic communication channel" (Kalakota and Whinston, 1996). The development of EPS has arisen in response to recognition of the weakness of traditional payment systems in the environment of modern commerce (Panurach, 1996). In general, there are two main types of EPS:

- (1) wholesale EPS, designed primarily for the business community's payment needs; and

- (2) retail EPS, designed primarily for the individual consumer of financial services.

Wholesale banking represents payment activities occurring at the corporate level (such as automatic salary payments to employees' bank accounts, direct company-to-company payments via banks, or international funds transfers. Retail banking represents any banking which is not wholesale-based and is generally focused on the personal sector, rather than on the corporate sector (Howcroft and Lavis, 1986). Figure 1 illustrates the range of EPS available today.

It is not the purpose of this paper to discuss this range of EPS in detail (but it is important to understand where Internet payment systems fit into the continuum of EPS; and how this sub-group of the wider EPS group differs from its fellows. The major difference between IPS and other EPS is that IPS use the Internet as amedium to transfer financial information, whereas the other EPS use private or government communications channels. It is also important to note that very often, card-based payment systems (such as credit, debit or charge cards), are also defined as retail-based electronic payment systems. These card-based payment systems are mainly used with other types of EPS to maximise the benefits of electronic banking. For instance, consumers are presently required to have certain types of card to be able to use ATMs and EFTPoS.

Security and privacy

Before considering various types of IPS, it is worthwhile to mention briefly two fundamental issues of IPS development (security and privacy). Security is a crucial prerequisite to successful IPS development, since prospective IPS users frequently mention their concern about security of payments and financial information, such as card numbers and details. Since the Web was originally designed to publish information, additional security features are essential for commercial usage (particularly where this involves transmitting payments (Loshin, 1996). Bhimani (1996) also argues that strong security for financial transactions should satisfy additional criteria, including:

- confidentiality;

- authentication;

- data integrity; and

- non-repudiation of the transaction.

Most current IPS ensure the security of Internet transactions by applying a variety of methodologies and techniques.

Why is the privacy issue important when considering IPS? As Internet commerce becomes a reality, rather than a dream, people will be able to obtain any goods and services through this new marketplace. People's purchasing patterns disclose a great deal about their lifestyle. If it is possible to trace back a person's purchasing records for the past year, there is little difficulty in then drawing conclusions about this purchaser's interests (with serious implications for their private life). Customers' privacy can only be protected if banks or merchants are not able to trace back their payments. There are various ways in which the privacy of Internet users can be protected - but there is a conflict between consumers' right to privacy and regulators' desire to prevent illegal financial transactions. While consumers want to retain their privacy, some government bodies and organisations want to be able to trace the transaction, especially when it involves illegal activities (Julian, 1996). The Cross-Industry Working Team (XIWT, 1996) suggested that the best resolution of these various concerns might be an "almost anonymous transaction", which means anonymity is maintained unless the customer gives permission, or a government warrant is issued.

Types of Internet payment systems

An important issue for any researcher into IPS is: "why has the development of IPS been one of the most interesting issues in recent years on the Internet; and why do so many organisations bother to develop new payment systems?" Fundamentally, the major reason for developing an IPS is that it provides organisations and consumers with a means of integrating individual commercial services into an electronic marketplace (or "market-space"), known variously as an "electronic market", "virtual market" or "on-line shopping" (Crede, 1996). In other words, the provision of Internet-based payments is the last major barrier to the Web's ability to provide a true market medium for electronic commerce. Lynch and Lundquist (1996) argue that electronic markets will benefit both companies and consumers:

- Companies will benefit from virtual markets because the concept of online shopping can make their business communication easier and cheaper.

- Consumers will benefit because on-line shopping is convenient and saves

time.

Of the more than 30 IPS proposals which have been published on the Web since the middle of 1996, some are from large corporations such as Mastercard, Visa, DEC, IBM or Microsoft, but a number were contributed by cryptography experts or by individuals or small firms specialising in Internet commerce. Most currentmodels of IPS proposals and schemes can be categorised as:

- third-party based systems (electronic cheque based systems and electronic clearing-house based systems);

- card based systems (credit card-based systems and smart card based systems);

- secure Web server based systems;

- electronic token based systems;

- financial EDI based systems; or

- micropayment-based systems.

It should be noted that proposals and schemes can often be grouped into more than one category (for instance, some smart card based IPS have also made use of the concept of electronic cash. In the following sub-sections we discuss these categories briefly.
Third-party based systems

The basic idea of this group of IPS is that of using third parties to establish trust between the two negotiating parties, by providing authorisation for both parties. The big advantage of this approach is that it truly provides a way of verifying the identities of the parties concerned, so that everyone can trust everyone else (Visa International, 1996). There are two main types of third-party based systems - electronic cheque based systems; and electronic clearing house based systems (credit card based systems could also be included in this category, but we preferred to separate this group into a category of its own in the interests of clarity).

The principle of electronic cheque based payment systems is similar to that of the traditional paper cheque, the only difference being that the cheque takes an electronic form rather than a physical, paper form (Mankin, 1994). Just like the traditional paper cheque, electronic cheques can bear the electronic equivalent of a signature which will authenticate the owner of the account (NetCheque, 1996). The real advantages of electronic cheques are that:

- they allow the user to specify the exact amount of the transaction; and
- the customer's money is kept securely in the bank (Richards, 1996).

First Virtual Holding is a company providing secure payment systems over the Internet by means of a third-party electronic clearing house system. The First Virtual IPS uses simple e-mail facilities and does not require additional software, hardware or encryption methods (First Virtual, 1994) (and differs noticeably from other IPS, especially those relying heavily on cryptography:

consumers must register their credit card details with First Virtual, using the telephone instead of the Internet to ensure security for the details,

to receive a VirtualPIN and become a member of the First Virtualsystem;

customers then give service providers their VirtualPIN to obtain services over theInternet;

- the merchant sends this VirtualPIN to First Virtual for verification;

- to complete the transaction, First Virtual will charge the debt to the customer's credit card account without involving the Internet.

First Virtual is safe, since actual details of the credit card are never transmitted over the Internet (Crede, 1996).

A different approach again is provided by CyberCash, which enables Internet commerce by providing a secure payment system over the Internet. The CyberCash secure Internet payment service guarantees the security of any financial transaction through secure communications between consumers, merchants and banks (CyberCash, 1996). Three separate programs are used to ensure security of the payments:

- (1) consumer software;

- (2) merchant software; and

- (3) operating software which is part of the CyberCash server.

The consumer's software is called the CyberCash Wallet and is the key component of the system:

- to make a payment using CyberCash, consumers must link their credit card details to wallet ID;

- once this link is complete, consumers can purchase any goods and services using their wallet ID;

- when wallet ID is transmitted as part of the purchase order to the merchant, the merchant adds additional transaction information to the received purchase order and sends this to CyberCash;

- CyberCash reformats this message and sends it to the bank for approval;

- when the payment is approved by the bank, CyberCash notifies the merchant;

- finally, the merchant will send an electronic receipt to the customer.

A total of 1,024-bit RSA and 56-bit DES encryption and digital signature features are used to secure messages during the payment approval process (CyberCash, 1996) which, according to Loshin (1996), takes only around 15 seconds to complete. CyberCash works with virtually all types of credit cards, electronic cheques and electronic coins (digital coins) and is compatible with all Web browsers and most server platforms. Crede (1996) believes that CyberCash is a more cost-effective payment system than credit card based systems.
Card based systems

We have used this term to refer to the simplest use of credit cards across the Internet (the direct use of a credit/debit card to pay for a transaction, although some proposals require special reading devices in order to transmit the payment directly over the Internet. The great

advantage of this approach is that it allows consumers to use their existing card in both off-line shopping and on-line Internet shopping (Visa International, 1996). It is also portable, since the cards are small enough to carry around to different places. There are two main card based IPS introduced in this section:

- (1) credit card based; and

- (2) smart card based systems.

Credit card based IPS simply require the provision of the purchaser's credit card details to the service provider for goods and services purchased over the Internet. There are, of course, some risks involved in sending such details over an unsecured Internet channel: primarily that someone can "hack" this message and copy the credit card details, which could then be used for criminal purposes (DigiCash, 1994). To overcome this problem, MasterCard and Visa co-operated to develop a technical standard for safeguarding credit card payments in February 1996 (MasterCard, 1995; Visa International, 1996). This new specification is called secure electronic transactions (SET) and ensures the security and privacy of personal and financial information by adopting digital signatures and public-key encryption technology. SET also uses digital certificate technology to verify the person at the point of sale, so that both parties can trust one another.

A major advantage of credit card based systems is their worldwide access and acceptability. According to MasterCard (1995), the number of acceptance locations is greater than 13 million and the organisation has partnership relations with 22,000 member financial institutions around the world. A commonly-known disadvantage is the high transaction fees associated with credit card use (unless credit card companies agree to reduce transaction fees to a much lower level, this approach would not be appropriate for micropayments).

The concept of "smart cards" (sometimes referred to as stored-value cards) is quite similar to that of stored-value phone-cards. Money can be downloaded into a small card by means of a read/write device (which can even be attached to a home computer) and the cardholder can spend this "money" anywhere, by inserting the card into a reading device at the point of purchase (Richards, 1996). Security is provided by a microchip, located inside the card itself. Another advantage of smart cards is that they can integrate into the existing network of ATMs so that cash can still remain the predominant form of payment transaction (Crede, 1996). To be able to make payments directly over the Internet you need special software and a smart card-reading device. Values contained in the card can take the form of cash or electronic cash (some IPS combine smart card-based systems with electronic cash based systems to increase security and portability for payments over the Internet.

The Mondex card is an electronic cash smart card. As Panurach (1996) explains, pure electronic cash can be very useful for network and Internet transactions, because it can eliminate money in its physical form. An important aspect of electronic cash is that the Internet requires new types of cash which can be easily recognised and accepted as physical cash for the electronic marketplace (Mondex, 1996). Mondex allows secure transactions since security is achieved by the chip on the card, rather than on unsecured networks. Mondex can also be used for micropayments, because the unit cost of transactions is relatively low. One major disadvantage of the Mondex card is that value can only be transferred between Mondex cards, which limits their applicability (Jones, 1996).

Secure Web server-based systems

The basic concept of a "secure Web server" is that both consumers and merchants use the same Web server, which is supported by a security protocol for the transfer of funds. The most well known security protocols are Secure HyperText Transport Protocol (S-HTTP) and Secure Sockets Layer (SSL) which were developed by Netscape (Loshin, 1996). These standards combine secure Web browsers with servers to provide a secure communication channel between vendors and customers (Ellsworth and Ellsworth, 1996). NetMarket argues that it was the first company to offer a secure commercial transaction on the Internet, in August 1994. The technology is based on a public-key encryption technology called pretty good privacy (PGP). NetMarket's encryption service was adopted by NCSA Mosaic to secure commercial transactions over the Internet, although this approach is becoming less popular for a number of reasons:

- one obvious reason is that both parties must use the same server to be able to transfer business transactions;

another argument is that this method does not provide a complete on-line service, such as checking validation and security for merchants in the Internet commerce environment, even though it can provide security for consumers. To satisfy both parties, it is necessary to link with existing authorisation networks (such as credit unions) and allow consumers to use alternative paymentmethods (Loshin, 1996).

Electronic token based systems

DigiCash is one of the leading companies in electronic cash-based IPS. Ecash is one of the products developed by DigiCash and is an electronic token equivalent to cash. According to DigiCash (1994), Ecash is designed for secure payments from any personal computer to any other workstation, over e-mail or the Internet. An important aspect of Ecash is that it provides better features than physical cash. For instance, Ecash is anonymous, hard to forge and prevents criminal usage. DigiCash ensures the security of financial transactions and the privacy of customers by applying public key encryption, digital signature techniques and blind signature

techniques which make use of cryptography (Crede, 1996). A disadvantage of the Ecash concept is that digital tokens are uninsured (for instance, if the customer's hard drive and the bank's system happen to go down at the same time (although this would be an extraordinary coincidence) there would be no way to reimburse the customer, since the bank does not link the money to the customer (Richards, 1996).
Peirce and O'Mahony (1995) proposed the PayMe Protocol Set, which supports both the anonymity and scalability of the IPS, supporting large numbers of users and multiple banks. The PayMe Protocol Set combines two technologies, DigiCash's Ecash and NetCash (developed at the Information Sciences Institute of the University of Southern California). An anonymous transaction is achieved by adopting DigiCash's Ecash technology (although the anonymity is limited since the address of the buyer's network will be known), while scalability is achieved by adopting the NetCash protocol.

Financial EDI based systems

Electronic Data Interchange (EDI) is the computer-to-computer exchange of business documents between organisations in standardised format (Swatman, 1993). Businesses and their vendors use EDI to exchange many business-related documents such as purchase orders, invoices, shipping notices, and payments to cut costs and run the business more efficiently.

Financial EDI involves the electronic exchange of financial documents such as payments and remittance advices in a standard format which computers can read (Bank of America, 1996). A number of organisations are trying to apply financial EDI systems over the Internet by simply using e-mail. CommerceNet, a well-known electronic community, has recently conducted a pilot test of financial EDI (CommerceNet, 1996), using the Internet's Simple Mail Transport Protocol (SMTP) to exchange messages, thus providing a much more rapid delivery time than traditional EDI networks can achieve. Security of messages is achieved by adopting two standards, Privacy Enhanced Mail (PEM) and Multipurpose Internet Mail Extension (MIME), which are both based on the public-private key technology patented by RSA Security, Inc.

Micropayment-based systems

Micropayments are small-value transactions and comprise the majority of payments on the Internet at present (Glassman et al., 1995), since many information goods (such as files and images) are relatively cheaper than physical goods. In previous sections, various IPS were examined and discussed, but few of them can actually support consumers in purchasing items costing fractions of a cent, or even items less than a dollar in value, because of their high transaction fees. There are a number of IPS specially designed to meet the requirements of micropayment, such as MicroMint, Payword, Millicent and Micro Payment Transfer Protocol (MPTP).

As an example of how these protocols work, Millicent is a secure protocol which was developed by Digital Equipment Corporation (DEC) to investigate the possibility of small-scale commercial transactions over electronic networks (DEC, 1996). Millicent cuts the cost of the transaction process by reducing additional communication, expensive encryption or off-line processing. Scrip and brokers are critical components of this system. Scrip represents an account which the customer establishes with a vendor. Each scrip contains the name of a specific vendor and the account's value (balance). Brokers maintain the accounts of customers and vendors; and handle all real-money transactions. Brokers expect the customer to have only a few dollars in a scrip at any time. Millicent assumes that keeping the value small and using a scrip only once will make this less liable to attack from criminals. Another aspect of security is that every transaction requires the secret number associated with the scrip, which is known only by the customer. Millicent also prevents any fraud on the broker's part, since customer and vendor software can independently check the balance of the scrip.

The rapid growth of the Internet since its commercialisation has provided the impetus for the many new Internet payment systems currently available or under development, because it became apparent very quickly that traditional payment methods would not suffice for this new electronic marketplace. In the early stage of IPS development security was the major concern, but most IPS developers easily and quickly overcame problems associated with securityby applying encryption techniques. At this stage, it is difficult to evaluate how reliable these IPS are because a payment system requires more than security alone to be really effective. The remainder of this paper will explain how we designed our research project to identify effectiveness indicators for IPS and evaluated the findings of our Delphi survey of IPSexperts.

Research methodology and design

The research project which this paper describes was intended to identify common effectiveness criteria for Internet payment systems. But before

these criteria could be identified, it was necessary to define two subsidiary objectives:

- (1) Who are the main parties involved with Internet payment systems?

- (2) What are the effectiveness indicators, according to each party involved in an Internet payment system?

After careful examination of several research methodologies, including in-depth case study and survey, we decided that neither was suitable (case studies would not give us a sufficiently wide range of opinion or experience; and mail-based surveys would provide information which was too superficial for our purposes). We decided instead to adopt the Delphi survey approach and to make use of expert opinion to assist in developing our criteria for a number of reasons:

- it gave us the opportunity to garner opinion from participants in a number of countries;

- it allowed participants to complete the questionnaires in their own time;

- the anonymity of the participants would prevent the dominance of any one member over the others;

- Delphi surveys produce precise, documented records (Hwang and Lin, 1987); and

- more importantly, perhaps, it enabled us to gain a reliable consensus of opinion from a group of experts, even though the research project was undertaken during a relatively short period (less than a year).

Research methodology

In the early 1950s, the term Delphi was used to describe a reliable consensus of opinion, obtained from a group of experts by a series of intensive questionnaires interspersed with controlled opinion feedback (Linstone and Turoff, 1975). This approach is characterised as "a method for the systematic solicitation and collation of judgements on a particular topic through a set of carefully designed sequential questionnaires interspersed with summarised information and feedback of opinions derived from earlier responses" (Delbecq et al., 1975,p. 10). Delphi is particularly useful when accurate information is unavailable or expensive to obtain, or where evaluation models require subjective inputs to the point where they become the dominant parameters (Linstone and Turoff, 1975, p. 10). The survey is the most common technique of Delphi application. Delphi surveys are specially designed to obtain the opinions of experts and such a survey has three special features:

- (1) anonymity of participants;

- (2) iteration and controlled feedback between rounds; and

- (3) statistical summary of group response.

Research design

A research design is a logically-designed plan which allows a researcher to derive appropriate conclusions from his/her initial research question (Yin, 1989). We came up with the following strategies for the research design, after defining the objectives of the project:

- the appropriate number of participants would be between 10 and 15 (a trade-off between having sufficient numbers to provide confidence in the results; and having few enough respondents to ensure that all participated fully);

- electronic mail would be used to communicate with participants;

since time was a limiting factor, it was most appropriate to have only two rounds ofDelphi survey;

- open-ended questions would be used for the first-round questionnaire, to allow participants to address broad problems and issues; and

- structured questions would be used for the second-round questionnaire, to obtain more precise and detailed results.

The main steps involved in designing a Delphi survey include: contacting participants; designing and sending the first-round questionnaire; producing feedback from the first round; designing and sending the second-round questionnaire; analysing the results of the second round; and preparing a final presentation.

Research findings

Delbecq et al. (1975) argued that the participants in a Delphi are individuals who have a deep interest in the issues; and important knowledge or experience which can be valuable for the study. Respondents included individuals considered to be experts in the field of IPS and who had agreed to participate in the Delphi survey. A total of 28 well-known and respected individuals and organisations were selected for initial contact through journals, Internet publications and recommendations by other respondents who had already agreed to participate in this survey. An invitation letter was sent to clarify the objectives and depth of the study (this letter is included in Appendix 1). After the initial contact, 19 participants agreed to participate in the Delphi survey. Respondents came from government agencies (Australia only), academics and researchers, the legal profession, banks (Australia only) and IPS providers and developers.

The first round
The aims of the first round were to:

- Define the major parties/groups which are directly involved in an IPS.

- Define the effectiveness indicators for an IPS from the point of view of each group.

The first goal was to identify the major parties directly involved in current IPS. Any sub-organisations or minor parties could be ignored, since the focus of this study was broad rather than being based upon particular party or group. The second goal was to find the factors that an IPS must consider to make the system really effective. The first round questionnaire sent to respondents included two open-ended questions:

- (1) In your opinion, what are the major parties directly involved with an Internet payment system? Please identify and discuss each of the parties in moderate detail.

- (2) When you consider an IPS, what effectiveness indicators/success factors do you believe need to be addressed in terms of each of the parties you have identified in question one above? Please include the definition or

term you are using for each indicator. Note that some factors are applicable to more than one party.

The final version of this questionnaire, which includes sample answers (see Appendix 2), was sent to respondents by e-mail. Out of 19 respondents who had agreed to participate in the Delphi survey, 14 completed the first round questionnaire.

Major groups involved with IPS

Responses from first round identified six major parties directly involved with IPS:

- Financial institutions including banks and non-bank financial institutions (NBFI). These are the parties which can be viewed as external Internet bodies who hold the initial real monetary value. Financial institutions (including banks, credit unions and finance corporations) are normally required to have a licence to carry out banking business. They are a key player, although some IPS provide services without the direct involvement of financial institutions. Payments must be cleared by financial institutions regardless of how much they are involved in the actual process of paying for the goods and services. Another important fact is that financial institutions in general have the monopoly on consumers' confidence regarding their money. To maintain their position as a centre for payments, financial institutions are taking advantage of the opportunity to develop collaboration between IPS developers and companies which rely on Internet usage for their business. Thus the development of the concept of the "Internet bank" can be realised on a large scale.

- IPS providers or manufacturers. These are the parties which operate and manage the IPS (and can vary from the provider of a single software package to a large organisation. In general, they are responsible for providing the IPS software and interfaces required by merchants and customers. Although some financial institutions provide direct IPS service (e.g. SET from MasterCard and Visa International), the IPS providers are generally third parties which establish transactions between financial institutions (banks and NBFIs) and end-users (merchants and consumers). At this stage, IPS providers still need to co-operate with financial institutions on a large scale to gain their market penetration and consumer acceptance.

- Merchants (vendors). These are the parties selling goods and services (both conventional and information-based) directly to consumers over the Internet, using an IPS to manage payments. Merchants' main requirement is for a reliable and low-cost IPS, since Internet vendors are often small companies with narrow profit margins. Their current involvement with IPS is very much dependent upon customer demand (at this stage, the majority of Internet merchants are adopting the IPS concept on a small scale at an experimental level, rather than fully adopting the system.

- Consumers. These are the end-users of the trade cycle who want to use the IPS to pay for goods and services which they purchase over the Internet. Consumers can be further categorised into end-users, commercial users and government users. Consumers are the most important group in any IPS (in fact, they are the people who must really be convinced to see the real advantages of using an IPS, because business has no meaning without the consumer. This is one of the problems for IPS providers. Although most IPS can provide secure transactions over the Internet, a large proportion of consumers still believe that making payments over the Internet is a dangerous activity. Apart from ensuring the security of their payments, consumers are also looking for IPS that are reliable, cheap and widely

accepted by a large number of merchants. They do not want to use ten different IPS to obtain different types of goods and service over the Internet.

- Regulators. This group includes national regulators (such as government bodies, law enforcement agencies, the legal profession and banking regulators). Regulators have a variety of reasons for being interested in IPS development, including the impact of the IPS concept on the money supply, ways of tracking tax payments in cyberspace and the need to protect consumer rights and the public interest. At this stage of IPS development, their dilemma is how to encourage the development of efficient IPS while also being able to protect the public interest. For instance, law enforcement wants to be able to trace back payment transactions to track illegal activities, but this requires consumers to sacrifice some of their entitlement to privacy.

- Network providers. These parties provide the physical support infrastructure for Internet payment systems, including IPS software, hardware and telecommunications facilities.

Effectiveness indicators for IPS

Restating question 2 from questionnaire 1 "when you consider IPS, what effectiveness indicators/success factors do you believe need to be addressed in terms of each of the parties you have identified in question 1 above? Please include the definition or term you are using for each factor and note that some factors are applicable to more than one party". In many responses, a large number of the same effectiveness indicators were applied to more than one group. The main reason given was that success factors for IPS primarily depend on customers' needs, so that some effectiveness indicators for IPS providers and financial institutions also depend on consumers' effectiveness indicators. The effectiveness indicators produced as a result of the first round include:

- Ability to allow refunds: merchants should be able to refund payments to clients if necessary.

- Ability to support both on-line and off-line activity: allows more flexibility to operate the system even when the network breaks down.

- Acceptability: IPS must be accepted at a wide variety of stores and banks.

- Accountability: transactions must be accountable.

- Anonymity: the ability to conceal the identity of the payee.

- Authentication: the ability to authenticate the users of the system.

- Customer support: the IPS should be able to assist customers electronically at minimum cost and throughout the day.
- Duration of transaction process: the time it takes to approve the payment (transaction delay must be minimised as far as possible.

- Ease of use (convenience): the IPS must be as convenient as cash to use on any occasion. Its software must also be easy to use (user-friendly).

- Exchangeability (also known as fungibility): funds must be easily exchangeable between parties.

- Flexibility: the ability to allow different kinds of IPS.

- Functionality: the need to increase the functionality of systems to gain competitive advantage over competitors.

- Irrefutability: the ability to ensure that the payments cannot be refuted or disproved.

- Legal certainty: payments made using an IPS must be legally accepted.

- Low fixed costs: costs (including set-up cost, equipment cost and infrastructure cost) must be reasonably low for consumers and merchants.
- Low transaction cost: cost of the transaction itself must be as low as possible (zero transaction cost is desirable if possible (just like a cash transaction).

- Portability (remote access): the ability to allow consumers to make payments from a variety of locations using a range of different interface devices.

- Privacy: the ability to maintain public confidence to ensure customer privacy.

- Profitability (cost-effectiveness): implementing the IPS must be profitable and cost-effective, especially from the merchant's perspective.

- Regulatory framework: the system must be able to operate in a regulatory framework that the regulators understand and can enforce.

- Reliability (trustworthiness): the IPS must be reliable, so that merchants and consumers will have confidence in using the system.

- Responsibility: the IPS must be responsible for any fraud, data security, or data privacy.
- Scalability: the ability to decentralise the system as much as possible to avoid bottlenecks.

- Security: the ability to protect the details of transactions and customers from internal and external fraud/criminal usage.

- Traceability: the ability to trace back the transaction, particularly in the case of illegal activities.

- Transferability: the ability to transfer value between customers.

- Universality: a global standard interface (allow use anywhere around the world).

- Unobtrusiveness: the ability to integrate the system into the user's daily life.

Anonymity and privacy are frequently treated as being identical. There is no doubt that anonymous payment can provide a perfect solution for consumer privacy, but this is the area in which the conflict occurs between regulators and the other parties. In this research project we therefore interpreted anonymity as being merely one of the ways of ensuring consumer privacy, which can also include protecting customer details (which must, of course, be protected from unauthorised access). Table I summarises the effectiveness indicators found for each group.

Other comments made by respondents led to some adjustments in the first round results :

- Initially, much research concentrated on making IPS anonymous. This is perhaps less important now than other factors. However, privacy should be maintained (it is desirable that parties outside the purchase transaction should not be able to obtain a customer's personal or financial details). Customer anonymity from the IPS is the least practical, but anonymity of the consumer from the merchant is feasible and would prevent unwanted targeted marketing by the merchant to previous customers.

- Effectiveness indicators for IPS might vary, depending on what consumers are looking for, the types of system being used and the level of government control. If consumers are looking for relatively small payments (say less than $1 in value), the speed of the transaction might be more important than the level of security. Conversely, if the payment is large (say more than $100 in value) security will probably be more important than the speed of the transaction.
- Some respondents found it surprising that profitability (cost-effectiveness) was not one of the effectiveness indicators for consumers. I believe that consumer cost-effectiveness can be identified as low transaction cost. Most IPS do not require consumers to spend a lot of money in setting up the system to obtain service - in fact, there are generally no IPS costs for initiating the system to access the Internet. What consumers need is to be able to open an account and install an IPS software package - and some IPS even provide free software for merchants and consumers. We therefore believe that the major IPS costs for consumers relate only to the actual service charge incurred for each transaction.

The second round

As the results of the first round show, the groups involved with all IPS were clearly identified and effectiveness indicators were defined for each of these groups. Since the first round questionnaire was designed to ask respondents to answer as broadly as possible, we found that the majority of effectiveness indicators were related to more than one particular group. These results did not, however, indicate which effectiveness indicators were more important for one particular group than for any others. This issue was the focus of the second round of the Delphi survey, which was: "to find what are the most important effectiveness indicator(s) for each group".

The second round questionnaire was developed and returned to the respondents, together with feedback from the first round. Questionnaire two asked respondents to rank all effectiveness indicators according to their importance for each group; and also asked them to explain the reasoning behind their selection of the three most important effectiveness indicators (see Appendix 3 for more details). We also asked respondents to make two further assumptions for the purposes of the second round survey, both of which were included in the interests of simplicity:

- (1) Consider small and medium-sized enterprises (SME) rather than large enterprises.

- (2) Consider direct payments from consumers to providers of goods and services.

Table II summarises the results of the second round Delphi survey. Each number represents the summation of the respondents' ranking of the effectiveness indicators for each group, that is, the ranking is based on

the number of responses which were given for each indicator. It is important to note, however, that all the effectiveness indicators identified in the first round are still critical components of an IPS. The result of the second round analysis shows which effectiveness indicators are more important than others at the current stage of IPS development. As IPS become more mature, these rankings are likely to change, just as they do in the case of any other payment system:

- The results clearly indicate that security and reliability (trustworthiness) are major effectiveness indicators for almost all groups.

- Financial institutions need to be able to authenticate individual transactions in terms of payer and payee, to avoid putting themselves at risk. They would also prefer that the IPS be able to integrate with existing private banking and clearing networks, instead of having to build and design complete new networks to be cost-effective.

- IPS providers and manufacturers should be able to distribute the system, if required to meet a certain level of service provision for clients. Bottlenecks in the system must be resolved, because these can lead to general dissatisfaction with levels of service. It is also important that these groups provide a system which can be widely accepted.

- Merchants are looking for an IPS which can provide low transaction costs, because high costs discourage consumers from using the system.

- Consumers are more concerned with security of their payment details and low transaction costs. To make an IPS attractive to consumers, it must not be more expensive than traditional payment systems (unless the system is so convenient that consumers are willing to offset the higher transaction cost against the convenience they receive.

- It is essential for regulators to be able to trace transactions for legal purposes and to prevent illegal activities. The biggest dilemma for regulators is that where transactions can be traced for legal purposes, they are less likely to be used for illegal activities; but such traceability can also be the major impediment to an efficient, effective policing of on-line purchases.

- Finally, from the network providers' perspective, an IPS should provide universality of the system to ensure maximum acceptance of different forms of IPS (it is not easy for network providers to set up different procedures for each IPS.

Conclusions

Since the Internet opened its gate to commercial use, a wide variety of commercial activities have moved into Internet-based operation. The Web, particularly, has become a most popular market medium for Internet commerce. By extending variations on traditional payment systems into this new electronic marketplace, consumers and organisations have begun to develop a number of new payment systems specifically oriented towards Internet commerce. In the early stage of IPS development, security was the biggest concern but most IPS developers easily and quickly overcame problems associated with security by applying a variety of technical solutions to encryption and delivery mechanisms.

This paper has reported on a research project which attempts to identify effectiveness factors for the various parties involved in Internet payments systems, using a Delphi survey to gain the views of recognised experts in the field and then building on these views to develop a set of criteria:

- the first round of the Delphi survey led to the identification of six principal roles for those directly involved with IPS:

- 1 Financial institutions (including bank and non-bank financial institutions).
- 2 IPS providers (manufacturers).

- 3 Merchants (vendors).

- 4 Consumers.

- 5 Regulators.

- 6 Network providers.

- At present, the consumer group is the key success factor for IPS success. However, for IPS to really take off, the six parties need to co-operate with one another and share the concerns (and, later, the benefits) of IPS provision. Effectiveness indicators for IPS vary depending on a number of factors, such as what consumers are looking for and what kinds of payments are being made. However, for the purposes of this study, general effectiveness indicators were identified for each group;

- the second round results show that security and reliability (trustworthiness) are the two most important effectiveness indicators overall;
- finally, different effectiveness criteria were developed for each of these six groups. In general, consumers are more concerned with security and privacy, while regulatory bodies want to have the ability to trace transactions to prevent illegal usage. Merchants, as one might expect, wished to provide systems which consumers would want to use, while IPS and network providers are most concerned with consistency.

There are, of course, many unresolved issues which need to be further discussed but which are outside the scope of this paper. These issues relate not only to technical aspects of Internet payment systems, but also to their political aspects (and include the following concerns:

- It is very difficult to produce universal IPS, because of differing tax and legal regulations. The Internet links the entire world and it is not owned by any single organisation or country. Should a legal dispute arise, it could be immensely complicated and protracted.

- How can a company impose a legal obligation on a customer using electronic ordering and payment?

- To what extent should anonymous payments be allowed for the consumer? Government agencies are responsible for managing the movement of money flow. They need to collect information about transactions in terms of managing customs duties and taxes.

- Anonymous payments raise another important issue, that of criminal money laundering. Hettinga (1996) stated that money laundering puts financial systems at risk and can lead to the corruption of entire societies. One clear argument made by Richards (1995) is that anonymous payments should only be allowed for small transactions, rather than large ones, to gain wide acceptance for the concept without running the risk of major fraud.

- What effect, if any, will the float generated by undetected counterfeit

electronic cash have on world trade (Julian, 1996)?

Research into electronic commerce is still in its infancy (these issues are extremely important and their resolution (or lack thereof) will have an important influence on how successful the Internet is as a commercial marketplace. This paper has attempted to identify those factors which most encourage effective and efficient Internet payment systems. While this research project was only a "pilot" for the development of such indicators, we hope that academic researchers and industry IPS developers alike will find them useful and will be able to base more detailed work on this foundation.

Note

1 Hyper-media is a form of multimedia, in which the "links" take users not only to other parts of the document itself, but also (potentially) to other parts of the Web - and thus to documents created by other users entirely.

References

1. Bank of America (1996, WWW document, URL http://www.bankamerica.com, accessed March.

2. Bhimani, A. (1996, "Securing the commercial Internet", Communications of the ACM, Vol. 39 No. 6, June.

3. CommerceNet (1996, WWW document,URL http://www.commerce.net, accessed April.

4. Crede, A. (1996 "Electronic commerce and the banking industry: the required and opportunities for new payment systems using the Internet", The Journal of Computer-Mediated Communication, Vol. 1 No. 3.

5. Cronin, M.J. (1996, Doing More Business on the Internet: How the Electronic Highway Is Transforming American Companies, 2nd ed., Van Nostrand Reinhold, New York, NY.

6. CyberCash (1996, WWW document,URL http://www.cybercash.com, accessed April.

7. DEC (1996, "Millicent: Digital's microcommerce system", WWW document,URL http://www.research.digital. com/SRC/millicent, accessed July.

8. Delbecq, A.L., Ven, A.H. and Gustafson, D. (1975, Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes, Scott, Foresman and Company, Glenview, IL.

9. DigiCash (1994, WWW document,URL http://www.digicash.com, accessed April.

10. Eager, B. and Pike, M.A. (1995, Using the World Wide Web and Mosaic, Que-Corporation..

11. Ellsworth, J.H. and Ellsworth, M.V. (1996, The New Internet Business Book, John Wiley & Sons Inc., New York, NY.

12. First Virtual (1994, WWW document,URL http://www.fv.com, accessed April.

13. Glassman, S., Manasse, M., Abadi, M., Gauthier, P. and Sobalvarro, P. (1995, "The Millicent protocol for inexpensive electronic commerce", 4th International WWW Conference, July.

14. Gray, M (1996, WWW document, URL http://www.mit.edu: 8001/people/mkgray/net/web-growth-summary.html.

15. Hettinga, R. (1996, "Internet banking and commerce: security", Journal of Internet Banking and Commerce, Vol. 1 No. 1.

16. Howcroft, J.B. and Lavis, J. (1986, Retail Banking: The New Revolution in Structure and Strategy, Basil Blackwell, Oxford.

17. Hwang, C.L. and Lin, M.J. (1987, Group Decision Making under Multiple Criteria: Methods and Applications, Springer-Verlag, New York, NY, Berlin.

18. Jones, T. (1996, "The future of money", Mondex publication, WWW document, URL http://www.mondex.com/ mondex, accessed June.
19. Julian, A. (1996, "The future of electronic cash", in Proceedings of EDPAC '96, Perth, Australia, pp. 14-17.

20. Kalakota, R. and Whinston, A.B. (1996, Frontiers of Electronic Commerce, Addison-Wesley, Reading, MA.

21. Krol , E. (1994, The Whole Internet, 2nd ed., O'Reilly & Associates, Inc.

22. Linstone, H.A. and Turoff, M. (1975, The Delphi Method: Techniques and Applications, Addison-Wesley, Reading, MA.

23. Loshin, P. (1996, Electronic Commerce: Online Ordering and Digital Money, Charles River Media Inc.

24. Lynch, D. and Lundquist, L. (1996, Digital Money: The New Era of Internet Commerce, Wiley Publishing Company, ch. 10.

25. Mankin, E. (1994, "The check is in the E-mail", USC Chronicles.

26. MasterCard (1995, WWW document,URL http://www.mastercard.com., accessed May.
27. Mondex (1996, WWW document, URL http://www.mondex. com., accessed June.

28. NetCheque (1996, "The NetCheque(SM) network payment system", WWW document, URL http://gost.isi.edu/info/ NetCheque, accessed September.

29. Network Wizards (1996, "Internet growth statistics", WWW document,URL http://www.nw.com, accessed August.

30. Panurach, P. (1996, "Money in electronic commerce: digital cash, electronic fund transfer, and Ecash", Communications of the ACM, Vol. 39 No. 6, June.

31. Peirce, M. and O'Mahony, D. (1995, "Scalable, secure cash payment for WWW resources with the PayMe Protocol Set", WWW document,URL http://ganges.cs.tcd.ie/ mepeirce, accessed April.

32. Poon, S. and Swatman, P.M.C. (1995, "The Internet for small businesses: an enabling infrastructure for competitiveness", in Kilnam C. (Ed.), Proceedings of the Fifth Internet Society Conference, Hawaii, USA pp. 221-31.

33. Poon, S. and Swatman, P.M.C. (1996, "Electronic networking among small business in Australia - an exploratory study", in Swatman, P.M.C.et al.

(Eds), Proceedings of the Ninth International Conference on EDI-IOS, Bled, Slovenia, pp. 446-60.

34. Poon, S. and Swatman, P.M.C. (1997, "Internet-based small business communications: seven Australian cases", in Proceedings of the 1997 PACIS Conference, Brisbane, Australia.

35. Richards, S. (1996, "Electronic banking resource center: electronic money/Internet payment systems", WWW document, URL http://www2.cob.ohio state.edu/ [similar]richards/bankpay.htm, accessed May.

36. Richards, T. (1995, Banking without Borders, Forex without Frontiers, WWW document, URL http:// www.hyperion.co.uk/pub/library/lib-bank.html.

37. Swatman, P.M.C. (1993, "Integrating electronic data interchange into existing organisational structure and internal application systems: the Australian experience", PhD thesis, School of Computing, Curtin University of Technology, Australia.

38. Visa International (1996, WWW document, URL http://www.visa.com, accessed May.
39. XIWT (Cross-Industry Working Team) (1996, "Electronic cash, tokens and payments in the national information infrastructure", WWW document.URL http://www.cnri. eston.va.us:3000/XIWT/documents/digcashdoc/ElecCash.html, accessed August.

40. Yahoo (1996, WWW document, URL http://www.yahoo.com.

41. Yin, R.K. (1989, Case Study Research: Design and Methods, revised ed., Sage.

Appendix 1: invitation letter

Dear

My name is Terry Tae-Hwan Shon. I am currently completing my Honours year in the Department of Information Systems at Monash University, where I am studying for a Bachelor of Computing (Information Systems) Honours degree. My research involves an analysis of efficiency criteria for Internet payment systems (IPS) - where IPS is defined as:"

any conventional or new payment system which enables financial transactions to be made securely from one organisation or individual to another over the Internet."

I have summarised the issues involved in a variety of existing IPS and from these issues developed a preliminary set of IPS efficiency criteria. I now need to validate my efficiency criteria and I am writing this letter to invite your participation in my study. I have selected a Delphi survey as the best way of obtaining such validation and hope that you will be prepared to participate in the Delphi.

Delphi survey is "a technique designed to obtain reliable consensus of opinion of a group of experts by a series of intensive questionnaires interspersed with controlled opinion feedback" (Turoff and Linstone, 1975). This technique is particularly useful where there are few reliable historical data or where accurate information is not available.

I hope to have two rounds of Delphi survey. The first round questionnaire is designed to ask more broad and open-ended questions. The second round

questionnaire will be designed on the basis of the result from the first round. (I expect to take much less time to complete the second round questionnaire than the first round.) Feedback to participants in the survey will be provided at the end of both rounds. The expected number of participants is between ten and 15 people and names of participants will remain anonymous.

Could you please reply to this letter by e-mail and let me know whether you are willing to participate in the Delphi survey? I know that some of the recipients of this letter have already been kind enough to agree by phone to participate in the study, but I would be very grateful to receive your written confirmation of acceptance.

Please do not hesitate to contact me if you have any queries regarding this study. I would also be most grateful if you could send me the names of any other people you believe would be suitable participants in a survey of this kind. Any comments or feedback you may have will also be of great use to me.

Best regards,

Terry (Tae-Hwan) Shon

Appendix 2: first round questionnaire (questionnaire 1)

First, thank you very much for agreeing to participate in this Delphi survey. Your name will remain confidential and all material circulated as a result of this exercise will be accumulated and shown only as total responses. This message contains the first-round questionnaire. For the purposes of this study I define term "Internet payment systems (IPS)" as "Any conventional or new payment system which enables financial transactions to be made securely from one organisation or individual to another over the Internet". Some examples of IPS are: CyberCash, Ecash(Digicash), FirstVirtual, SET, Mondex, Millicent, etc.

Q1 In your opinion, what are the major parties directly involved with Internet payment systems? Please identify and discuss each of the parties in moderate detail (a maximum of half an A4 page for each party), e.g."

(1) Financial institutions, IPS providers, merchants and consumers.

(2) Users, issuers and regulators.

Q2 When you consider IPS, what effectiveness indicators/success factors do you believe need to be addressed in terms of each of the parties you have identified in question one above? Please include the definition or term you are using for each factor and note that some factors are applicable to more than one party. To assist you in the task, I have provided a list of effectiveness indicators identified from the literature:
Flexibility, ease of use, cost-effectiveness, fungibility, universality, security, privacy, anonymity, reliability (trustworthy), low fixed cost, acceptability, portability, scalability, low transaction cost, transferability, obtrusiveness, duration of transaction process.

Sample answer. Financial institutions: flexibility (ability to allow different kinds of payment mechanisms); scalability (ability to decentralise systems as much as possible to avoid bottlenecks); IPS providers: scalability (ability to decentralise systems as much as possible to avoid bottlenecks). Merchants: fixed cost (costs of hardware, software, opening account and annual account cost); flexibility (ability to allow

different kinds of payment mechanisms.Consumers: fixed cost (costs of hardware, software, opening account and annual account cost); anonymity (ability to hide identity of payee); scalability (ability to decentralise systems as much as possible to avoid bottlenecks); fixed cost (costs of hardware, software, opening account and annual account cost); anonymity (ability to hide identity of payee).

Q3 Any other comments.

Appendix 3: second round questionnaire (questionnaire 2) - Introduction
Second round questionnaire

Introduction

Please rank the following effectiveness indicators according to their importance. Please state why you believe the top three indicators are more important than the others (writing your answers at end of each section).

Note: some respondents argued that the importance/preference of the effectiveness indicators will depend on what sort of business is involved, what customers are looking for, etc. For instance, if the value of the transaction is less than $1, the transaction process will be more important than security. I would therefore ask that for the purposes of the present survey :

- (1) Consider small and medium sized enterprises (SME) rather than large enterprises.

Caption: Figure 1; Types of electronic payment systems; Table I; Effectiveness indicators for Internet payment systems; Table II; IPS effectiveness indicator ranking

?

09603127

WIDE RANGE OF BUSINESSES CHASE A BOOMING MARKET SHARP GROWTH DRAWS INVESTMENT INTO A COMMERCE BUILT ON DISLOCATION, POVERTY

San Jose Mercury News (SJ) - Monday, April 13, 1998
By: MICHELLE LEVANDER AND RICARDO SANDOVAL, Mercury News Staff Writers
Edition: Morning Final Section: Front Page: 13A
Word Count: 1,128

MEMO:
Lost in Transit
RELATED STORIES: pages 1A and 13A

TEXT:
In a post-NAFTA world, a booming multibillion-dollar industry has grown up on the backs of the most humble players in the international economy: migrant workers.

Today, a host of new players are scrambling for a share of the lucrative business wiring money home, which is growing by 15 to 20 percent a year.

Banks, small regional money-wiring services and even the U.S. Postal Service, with its Dinero Seguro (Safe Money) program, entered the fray in the 1990s as Mexican immigration swelled to record numbers. Two Mexican state governments -- Jalisco and Guanajuato -- also are creating programs to make it cheaper to wire money and to encourage investment in migrants' home states.

Last year, Mexican immigrants sent home an estimated $6 billion, and about half that was in wire transfers. Such remittances could grow as high as $10 billion by 2000, predicts an official with the Mexican bank BanCrecer, although other projections point to $7 billion.

''It's a big block of money. Everyone wants a piece of it,'' said James F. McCabe, president of Bank of America Mexico.

Rapid change coming

''The old days of sleepy competition and costly traditional forms of sending are going to be very rapidly done away with,'' predicts Raul Hinojosa, director of the North American Integration and Development Center at the University of California-Los Angeles. ''New technological innovations will have a profound, revolutionary effect on the way that money has been sent.''

The payoff is enormous for even a small share of this commerce built upon dislocation, migration and poverty. Today, immigrants worldwide send home an estimated $50 billion to $70 billion a year.

''The business outlook is pretty healthy and solid because there is more movement by people out of the trouble spots of the world, more dislocation and shifting,'' said Stephen McClellan, an analyst at Merrill Lynch. ''People want to wire money to those who couldn't get out.''

The remittance industry is so attractive that subsidiaries of Transamerica Life Insurance Corp. paid at least $30 million in February to acquire a 21 percent stake in MoneyGram Payment Systems Inc., the

second-largest player in Mexico. Meanwhile, MoneyGram has been busy expanding into the money-order arena, paying $15.6 million last month to buy the money-order business of Mid-America Bank.

''It's a very profitable business,'' said Manuel Somoza, marketing director for the new money-wiring arm of BanCrecer, which started in a high-immigration suburb of Chicago. ''Your risk is minimal. It's all cash. You aren't loaning or lending.''

To compete in this exploding sector, businesses must attract consumers who lack bank accounts, credit cards, loans or any other ties to mainstream financial institutions. One Mexican player, consumer retailing giant Elektra, calls it ''banking for the poor.''

Elektra built its $800 million chain by combining its consumer-appliancesbusiness with counters for industry leader Western Union Financial Services Inc. Now Elektra is adding banking services and lending offices.

''Our clientele doesn't like banks. The people are intimidated by all the marble, the formal atmosphere and the impersonal staff,'' said Pablo Collado, Elektra's director of investor relations. ''These people feel comfortable in an Elektra store. . . . Our employees come from the same communities as our customers.''

So foreign are these consumers to mainstream financial institutions that bank officials from both countries are meeting with anthropologists to understand this immigrant population.

Leo Estrada, a Los Angeles demographer, told of one session with officials from a major California bank, which he would not identify. He said the bankers struggled with ''how regular bank customers would feel having poor Mexicans ask for money orders next to well-heeled people.'' Ultimately, the bank opted for a program that encouraged its immigrant customers to use the phone for their transactions.

But other companies are reaching out. Some Mexican banks that once shunned rural campesinos as clients are setting up special accounts so their families in the United States can send money home.

Wells Fargo venture

Banamex, or Banco Nacional de Mexico, Mexico's second-largest retail bank, has teamed up with Wells Fargo to offer an account that costs $10 to open and lets U.S. immigrants wire up to $1,000 a day.

For now, however, all the new competition hasn't translated into better deals for consumers, said Gail Hillebrand of the Consumers Union in California.

''We still think it costs too much to wire money,'' she said. ''We'd like to see competition on price, which we aren't seeing yet.''

Still, some competition has brought undeniable improvements.

For much of this century, Mexican immigrants wired money home in much the same way their grandparents did: slowly and inefficiently through a system plagued by corruption and theft.

All that changed five years ago when Western Union, faced with its first real competition from rival MoneyGram Payment Systems Inc., launched its

''Money in Minutes'' service to retail outlets throughout Mexico.

Before that, Western Union wires arrived only at the national telegraph offices, which were plagued by corruption and inefficiency, said one industry official.

''Western Union did it for a hundred years and it wasn't a very good service,'' said Warren Bechtel, a MoneyGram official who formerly represented Western Union. A Western Union official declined to comment.

Will prices fall?

Since then, reliability has become a major advance in the industry. Some believe better prices could be next.

MoneyGram recently announced plans to expand its $10 service fee for wiring $300 -- it had been $25 -- from a few border states to the rest of the United States.

But while service fees have come down, Hillebrand and other consumer advocates say exchange rates -- a hidden cost -- must become more favorable before consumers truly benefit from competition.

Some industry insiders and analysts predict service fees will drop further. A BanCrecer official predicts that although the money-wiring industry will remain lucrative, prices -- and profit margins -- will drop by 65 percent in the next two years.

Others are skeptical. McClellan of Merrill Lynch said Western Union, with 55 percent of the U.S.-to-Mexico market, has such an iron grip on the global market that no one could seriously take it on.

Western Union's dominant position was secured last fall when its parent company, First Data Corp. of Dallas, acquired low-cost rival Orlandi Valuta.

In 1995, the U.S. Federal Trade Commission broke up a mega-merger between industry giants Western Union and MoneyGram, which was shed by American Express. Although it cited worries of monopoly control then, the FTC gave itsblessing to First Data's marriage of Western Union with Orlandi Valuta.

CAPTION:
Photo, Chart

PHOTO SERGIO DORANTES -- SPECIAL TO THE MERCURY NEWS
Mexico's Elektra appliance chain has branched out into financial services it calls ''banking for the poor.''
(980413 FR 13A 2)

?

01386565/9
DIALOG(R)File 15:ABI/Inform(R)

01386565 00-37552
Making payments on the Internet
McAndrews, James J
Business Review (Federal Reserve Bank of Philadelphia) PP: 3-14 Jan/Feb 1997 CODEN: FRBPBN ISSN: 0007-7011 JRNL CODE: FRB
DOC TYPE: Journal article LANGUAGE: English LENGTH: 10 Pages
SPECIAL FEATURE: References
WORD COUNT: 5504
GEOGRAPHIC NAMES: US

DESCRIPTORS: Electronic commerce; Internet; Computer security; Payment systems; Regulation
CLASSIFICATION CODES: 9190 (CN=United States); 5250 (CN=Telecommunications systems); 5140 (CN=Security); 4310 (CN=Regulation)

ABSTRACT: To flourish as a marketplace, the Internet needs a means of payment. The challenge is to devise ways to protect against theft while conveying payment information that is recognized as authentic. Most payment services on the Internet use some form of public key/private key encryption, but others safeguard financial information in other ways. With a trusted-3rd-party method of payment, a customer authorizes the trusted 3rd party to make payments on his/her behalf. Another method of payment is digital cash, which is stored on a computer's hard disk and is electronically transferred to a payee. Digital cash systems typically propose to prevent counterfeiting by virtue of the issuer's digital signature on the digital cash, which verifies its authenticity. For the proposed payment systems, issues such as consumer protection, disclosure and assignment of participant liability and privacy are being addressed by regulators and law makers. Recently, the Federal Reserve suggested that stored-value-cards that can store no more than $100 be exempted form the provision of Regulation E, which governs many conventional electronic methods of payment.

TEXT: The Internet has begun to make the idealized marketplace discussed in economic textbooks seem more plausible. It allows low-cost, speedy, convenient, and informative communication across the world. However, to become an active market in goods and services the Internet must overcome a fundamental hurdle: a way must be devised for buyers and sellers to securely and conveniently exchange payment over the Internet. Software companies and financial institutions are now developing methods that will allow people to pay on the Internet.

A review of these efforts reveals the importance of security, authenticity, and privacy, which are often overlooked or taken for granted in other instances of making a payment.

Money is an ancient human artifice. For approximately 3000 years coins have been minted in India and Greece. Minting coins for use as media of exchange was a significant improvement over the alternative: exchange of metals by weight for purchases. Coins made a particular amount and quality of metal easily recognizable and hard to counterfeit. Milling the edges of coins made the practice of removing small amounts of metal from the coins very easy to detect. The creation of banks of deposit and their vaults made safeguarding coins easier.

Hence, coins became readily identifiable and transferable, attributes that raw metals did not possess. These attributes made trade easier. Our society is grappling with ways to create, once again, a way to make payments in a new medium: the Internet. The designers of Internet means of payment have the same concems that occupied mints centuries ago: how to make the proposed means of exchange easy to recognize and authenticate, but hard to counterfeit and steal. Today's designers work with powerful mathematical means of encryption, which can serve the same roles for Internet payments that minting coins served for earlier payment systems.
Several attributes of a successful medium of exchange-one of money's primary roleshave emerged over the centuries. Money should be identifiable, divisible, easy to transfer (both technologically and in the sense of there being widespread acceptance), and easy to protect against theft. The attempts to create successful media of exchange over the Internet reveal the importance of these attributes as well as the difficulties of successfully designing a system with those attributes.

THE INTERNET

The Internet, a network of computers that use a common method of communication, has experienced rapid growth in recent years. While estimates of Internet size and usage are imprecise, one estimate shows that the number of computers linked to the Internet increased from 213 in August 1981 to 3,864,000 in October 1994 and to 9,472,000 in January 1996. The amount of message traffic across one part of the Internet is estimated to have grown from 85 million packets in January 1988 (a packet is approximately 200 bytes; a byte holds one alphabetic character) to more than 60 billion packets in January 1995.1 The Internet is used to send mail, to transfer files, and-using the World Wide Web-to transmit graphics and sound.2
The impressive growth of the Internet has been facilitated to some extent by the steadily declining cost of computers. Furthermore, in many cases, individual users of the Internet (or their employers or sponsoring organizations) pay a fixed fee, or a fee that does not vary with the number of sites from which they gather information, and there is no marginal fee for the use of the network facilities in sending or receiving information. This zero marginal cost of usage makes sending a message across the country essentially free for many users.

The Internet differs from telephone networks in that each message does not have a circuit dedicated to it. Instead, a message on the Internet is divided into packets, each with the address of the message attached to it, and the individual packets are sent through computers (known as routers) to their destinations. This packet switching method allows many packets to simultaneously share the physical telecommunication lines across which the packets travel. This greatly economizes on the use, and therefore the costs, of telephone lines, relative to telephone calls, which use a circuit switching method that dedicates a circuit to a particular call.3

This inexpensive and increasingly ubiquitous form of communication and information transmission has made it possible to imagine continuous, worldwide electronic commerce. On the Internet, one can comparison-shop, read warranties, establish accounts, view images of products, and order goods and services from companies located anywhere in the world. Home shopping on the Internet could reduce the transaction costs of shopping significantly; many believe that it is the "killer app" of the Internet.? To flourish as a marketplace, however, the Internet needs a means of payment, but payment over the Internet faces some unique barriers. In particular, the challenge is to devise ways to protect against theft while conveying payment information that is recognized as authentic.

CAN I PAY WITH A CREDIT CARD OVER THE INTERNET?

When I make a phone call to my favorite mail-order catalog to order a pair of shoes, the only parties to the call are the order taker and me. If I were to send an e-mail over the Internet to the catalog company instead, the information may be routed through many computers not party to the transaction before it reaches the merchant, allowing others to intercept my message. If my credit card number is included, others can steal it. Furthermore, if a hacker has infiltrated either the merchant's computer network or the one of my Internet access provider, the hacker could intercept, read, and alter messages. Because of that, I can't be sure that my messages haven't been read or altered after I've sent them. The activity of intercepting and reading others' messages is known as snooping. While telephone fraud is a big problem, the ease with which criminals can fake e-mail messages of others-someone with sufficient knowledge of computer systems can connect to the victim's mailserver on the Internet and send the fake message from it (an activity known as spoofing)-makes enhanced security a necessity. It is also much easier for criminals to establish untraceable computer accounts to fraudulently collect credit card numbers (if they were unencrypted). It is much more difficult to do so with telephone mail-order operations.

The real possibility of theft of the information has precluded the widespread use of unencrypted credit card numbers over the Internet. Furthermore, the ease with which criminals can adopt fraudulent identities and untraceable addresses on the Internet deters people from attempting to purchase items over the Internet. Therefore, new means of making payment must be devised.

Designing a method of Internet payments, therefore, requires attention to two features of money that are necessary to securely convey payment information. Authentication of messages is important for both parties to a transaction. Finding a means to prevent eavesdropping is important, so that criminals cannot steal payment-related information, such as credit card numbers, as they are transmitted over the Internet. It may be that secret coding of information can solve both of these problems.

ENCRYPTION

As with all types of money, identification and recognition are necessary before a seller will accept a payment. Payment systems today use various means to identify a payer. In credit card transactions conducted in person, possession of the card and a signature matching the one on its back suffice. For point-of-sale transactions with a debit card, possession of the card and a password identify the account holder. When paying by check, a signature (and often a photo identification card) is necessary. For cash transactions, the currency is examined to authenticate it.

On the Internet this means that correctly identifying the customer and maintaining the integrity of the information are vital. A password-even one that has been encoded by some encryption device-is not enough to identify a person if it is used more than once (because of the possibility of theft of the password). If an encoded message is used more than once, it could be duplicated and sent by some other person posing as the original sender.

None of the measures used to authenticate the means of payment today are foolproof. Counterfeit currency and check and credit card fraud are significant problems. But the ease with which snoopers can intercept unencrypted messages has led security experts to believe that encryption of

financial information is necessary to approach the levels of security that people now enjoy with cash, checks, and routine credit card payments.

Privacy. Securing the integrity of a message sent on the Internet poses a difficult problem. Even when a message is encoded, if criminals were to decode the message, or steal the "key" by which the original message was encoded, the integrity of the message would be lost. With traditional encryption methods the sender and receiver have to share the key to successfully encrypt and decrypt a message. Therefore, the sender has to give the key to the receiver in some way. This makes the management of the secret key extremely difficult because it is much more likely to be stolen as it is shared with many parties (for example, all the merchants that accept a type of credit card) and as it is being communicated to all the parties to a message. Furthermore, with traditional methods of encryption, once someone has stolen the key, messages can be both decoded and encoded. Hence, a criminal, armed with the key, can pose as a legitimate party to the encryption system, and no one could detect the deception.

A new type of encryption was discovered in the 1970s by Whitfield Diffie and Martin Hellman, two American mathematicians. Their contribution to encryption theory was to recognize that systems of encryption can be created that use a pair of keys, one to encrypt the message and another to decrypt it. One type of these "asymmetric" cipher systems is a "public key/private key"cipher (commonly referred to simply as a public key cipher) in which the encrypting key need not be kept secret to ensure a private message.5 The decrypting key (the "private key") need never be shared with anyone else and, therefore, is much less susceptible to theft. (See Keys to Establishing Trust in Cyberspace.)

Under public key cryptography, if two people wish to exchange private messages, they each create a pair of public and private keys. Alice obtains Bob's public encryption key, uses it to encrypt a message to Bob, and sends it to him. Bob can then decrypt it using his private key. Only someone who has Bob's private key can decrypt messages encoded with his public key. To reply, Bob obtains Alice's public key, encrypts a message, and sends it to Alice. She deciphers the message using her private key. This system of encryption offers a great deal of security in managing the private keys because they never have to be shared with anyone. Clever applications of this type of cryptography can be used to verify identity (using a "digital signature"), authenticate messages, and provide a record of when a transaction occurredall vital aspects of a trustworthy means of payment on the Internet.
Encryption of electronic financial information traveling across the Internet offers a safeguard against theft of information, and the digital signature offers a way to authenticate the message. Hence, these sophisticated mathematical devices play the roles that other devices that prevent the theft of money-such as vaults, wallets, and commonsense security precautions-and devices that authenticate money-such as watermarks, specially printed paper, passwords, telephone authorization, and signatures-play in other forms of money.

APPROACHES TO INTERNET PAYMENTS

There are currently several approaches to offering payment services on the Internet: credit-card-based systems (which represent an extension of credit by the issuer of the credit card to the holder); payment orders (much like a check is an order to one's bank to make payment); or a new form of payment, digital cash.6 Most use some form of the public key/private key encryption system, but others safeguard financial information in other ways.

Trusted Third Party. At least one firm offers a trusted-third-party method of payment: a customer authorizes the trusted third party to make payments on her behalf. In such a system the customer supplies (over the phone or through the mail) the trusted third party with her credit card number or a voided check and written authorization to effect payment on her behalf. The customer is supplied with a password. As the customer orders a product over the Internet, she supplies the seller with her password; the seller reports this to the trusted third party; and it, in turn, sends to the customer a report of the transaction and asks the customer to confirm it. Once confirmed, the trusted third party conveys the payment information through the automated clearing house system (the electronic interbank system that banks use to exchange small-value payments). This system avoids the problem of eavesdropping, which is a concern in transmitting payment information across the Internet.

The trusted-third-party method offers the benefit of securing credit card or checking account information against theft. It requires, however, sellers as well as buyers to accept payment by the trusted third party; therefore, widespread acceptability is a potentially difficult hurdle for the system. As in all the systems we discuss, the security of the system itself is vital. Such security requires electronic firewalls that cannot be breached by a hacker.

Digital Cash. At least one firm is offering customers the ability to make payments in "electronic," or digital, cash, and others plan to do so.7 Digital cash consists of messages that use a sophisticated set of variants on the public key/private key encryption system. It is stored on a computer's hard disk and is electronically transferred to a payee. It may also be electronically replenished by transfer from one's account at a participating bank. A digital cash system employs software held by the participating financial institutions, their customers, and merchants. Using that software, the customer creates digital messages that are authenticated by the issuing institution in a way that third parties can recognize. The issuer's authenticated message is returned to the customer and acts as a substitute for cash. Amerchant that receives the digital cash can send it on to its bank and have its account credited or it can spend the digital cash.

Digital cash systems typically propose to prevent counterfeiting by virtue of the issuer's digital signature on the digital cash, which verifies its authenticity. Issuers intend to prevent double spending of the cash by "reissuing" or replacing digital cash each time it is spent; participating financial institutions will not accept cash with serial numbers that indicate it has already been spent.

Digital cash has the potential for a feature many believe is increasingly important in an electronic information age: anonymity In principle, the merchant need not know who is spending the digital cash it receives: the cash is authenticated by the bank, not the customer. The merchant might sell an item and be directed to send it to a computer account (if it is a piece of information that can be sent over computer networks) or to a post office box, not knowing who requested it. If the merchant is paid in digital cash and does not know the identity of the holder of the computer account, there is no way the merchant can find out the identity of the buyer.8

The concern for privacy is increased today because of the greater ease of compiling information electronically. Many firms sell information on their customers to other organizations for marketing purposes. The enhanced

privacy that is possible in a digital cash system comes at a cost of more complex software to run the system.

Credit Card Methods. Visa International and MasterCard announced on February 1, 1996, that they have agreed to jointly develop a standard to solve the problems of snooping and spoofing. American Express later joined the effort as well. The standard is called secure electronic transactions (SET), and it is based on public key cryptography. The developers of the standard will attempt to ensure the integrity of credit card numbers that a cardholder sends to a merchant by encrypting the numbers. Prior to any transaction, however, the developers of SET propose to verify the identity of both merchant and cardholder by having either the bank that issues the card (in the case of the cardholder) or the merchant's bank that processes the transaction (in the case of the merchant) provide both parties with "digital certificates." These certificates may bear the digital signature of Visa or MasterCard or some certifying authority (see Keys to Establishing Trust in Cyberspace). Verifying that the digital certificate does indeed bear the digital signature of the expected certifying authority should help to assure the cardholder that the merchant has a legitimate relationship with a bank and is therefore not attempting to fraudulently collect credit card information for later criminal use. Furthermore, the proposed design for SET seeks to ensure that the merchant will not be able to decrypt the holder's card number; rather authorization from the merchant's bank will ensure payment, and the consumer's number will remain unreadable to the merchant.

Prior to their February announcement, Visa and MasterCard had embarked on creating separate standards for securing credit card transactions on the Internet. The subsequent decision to join forces to create and adopt a single standard will simplify the process of using the software that will operate the standard. With a single standard a merchant will be able to identify itself and secure its payment information using only one system. The decision to jointly develop the system avoided a potentially costly duplication of effort on the part of the card associations, banks, and merchants.

Internet Banking. At least one bank exists primarily for banking on the Internet: it has only a small physical office, but a "virtual branch" on the Internet. While this bank does not offer a direct method of payment on the Internet, it allows its customers to pay bills by writing checks or making an electronic payment through the automated clearing house. This method is a variant of trusted-third-party payments because information flows through private interbank networks.

Other banks and technology companies have created the Financial Services Technology Consortium. This group is sponsoring research into electronic commerce over open networks, such as the Internet. One of their ventures is the electronic check project, an attempt to create a payment method that will be accepted much as a paper check is today. It, too, proposes to rely on encryption to secure account numbers and digital signatures to verify identities, but it will provide access to one's bank account, rather than create digital cash.

ACCEPTANCE OF THE NEW MEANS OF PAYMENT

There are many approaches to payment over the Internet. Will they all survive? It is too early to determine whether the different means of payment are useful and cost-effective, but as in non-Internet-based payments, it may be that different forms of payment may survive for different uses and for different users.

Many competing and complementary means of payment exist today. For example, while credit cards are useful for international and many retail and mail-order transactions, only some merchants are able to accept credit cards (that is, they are "signed-up" customers of banks' credit card services). Nor do all consumers have sufficiently high credit ratings to obtain a credit card. Credit card payments are relatively costly to make because they involve an extension of credit by the issuing bank. Furthermore, credit cards typically are not useful for paying a friend. Checks, while convenient for payments to individuals, are not as useful for international transactions. Checks are also fairly costly because of the care that must be taken in routing the paper check through the banking system and back to the one who wrote the check. Cash is convenient for low-value purchases and can be used anonymously in some circumstances, but it is costly to hold in inventory

Many foresee demand for a way to make very low-value payments over the Internet. For example, a person may wish to purchase a photograph of a movie star for $0.50. For such small payments it is costly to write a check or to use a credit card (which usually requires a minimum payment of about $20 because of relatively high cost per use). Typically, one uses cash for such a small payment. Hence, digital cash, if it proves sufficiently convenient and low cost, would be much in demand for low-value payments. The cost of a digital cash system is not yet known. Until such a system is operating on a fairly large scale, it is not certain that it can be operated at a sufficiently low cost to make payments for, say, less than a dollar economical.

Credit card methods may prove useful for larger dollar amounts on the Internet. People may be discouraged from using digital cash for large-value payments because they enjoy less float when using digital cash-a debit method of payment-than when using a credit card. Furthermore, many credit-card holders already use their cards to make payments by phone and may therefore be more willing to make the leap to using them over the Internet.

Privacy and security concerns may induce some people to use the trusted-third-party method of payment as well as digital cash. Both of these methods avoid sending credit card information over the Internet, even in a highly secure encryption scheme. In addition, a consumer may wish to withhold his identity from a merchant to avoid having the information used either for marketing purposes or by law enforcement agencies if he is engaging in illegal activities.

PUBLIC POLICY CONSIDERATIONS

The ways that payments are made in the United States today are governed and supported by law and public policy For example, the laws, policies, and contracts that govern the rights of the various parties involved in a check transaction are well established. These policies help to make checks a reliable and predictable method for making a payment for all the parties involved in the checking system.

For the proposed Internet payment systems, issues such as consumer protection, disclosure and assignment of participant liability, and privacy are being addressed by regulators and lawmakers. The resolution of these policy issues will affect the development and acceptance of the proposed systems.

In particular, questions about the degree to which disclosure requirements, account statements, and some form of electronic receipt would be useful and

appropriate for Internet payment systems remain largely unanswered. Required disclosure of liability can help inform parties to a system about their responsibilities and thereby improve decision-making, although such disclosures impose an administrative cost on the system's operator, which, if the system is to succeed, will be collected in some way from the consumers of the service. Account statements and electronic receipts would assist users of payment systems in reconstructing their activities in case there were questions about unauthorized use of their accounts or unauthorized payments-again, at a cost of record-keeping for the system and its users. Resolution of these issues will clarify the obligations of the parties and, with a careful balancing of the costs and benefits involved, will advance the development of acceptable forms of payment systems on the Internet.

Recently, for example, the Federal Reserve suggested modifying some provisions of its Regulation E, which governs many (conventional) electronic methods of payment, as it applies to stored-value cards.9 The Board's proposal suggested that cards that can store no more than $100 be exempted from the provisions of the regulation, and it makes further exceptions for various specific types of cards. For example, under the proposal, a merchant would not be required to issue paper receipts when certain types of stored-value cards are used for payment. Furthermore, in the proposal the Board also recognized that stored-value systems (such as various digital cash systems) are being developed for the Internet: "Systems are being proposed, for example, for making payments over computer networks, such as the Internet"; it also requested comments on the extent to which the Board should consider applying Regulation E to "various types of network payment products."

Another legal and contract issue is that, on the Internet today, the merchant (and the system operator and the consumer, for that matter) has no standardized or generally accepted and enforceable way to verify the signature or password of the other party to the transaction. As a result, the liabilities of the parties are unclear in the event of a repudiation of a transaction by a customer when the transaction was authorized using the customer's digital signature. In contrast, the assignment of liability in a credit card or (off-line) debit-card transaction is well established. The credit card associations were instrumental in standardizing the form of the contracts used today in the credit card industry. If Internet payment systems not based on credit cards are to succeed, such an association may be helpful in organizing contracts and standards that would form the basis for widespread merchant and bank acceptance of the systems.

A widespread acceptance of contractual standards that make the digital signature of the customer binding may be desirable to address the issue of how liability is to be assigned in the case of a repudiated payment.lo This issue is complicated by the fact that the federal government has chosen a standard for digital signatures that is different from the standard that has emerged in private industry. Neither has the force of law behind it. Recently, two states, Utah and California, have passed laws giving digital signatures the same validity as handwritten signatures. Similar legislation is pending in other states. These laws should reduce the possibility for repudiation and thereby advance the development of systems using digital signatures.

A second issue regarding digital signatures is who should be allowed to be a certifying authority for the public key used to create such signatures (see Keys to Establishing Trust in Cyberspace for a description of the role of a certifying authority for public keys). The certifying authority in granting a certificate to a party, puts its stamp of approval on the

certificate holder's management of the private key and provides the certificate holder a proof of identity. Such certification may carry an implicit guarantee of performance and hence may require the certifying authority to bear a considerable amount of risk. The authority may therefore require considerable oversight power for those to whom it grants a certificate.
Digital cash also entails policy considerations. The creators of digital cash envision individuals transferring it among themselves with no intermediary, which raises the issue of what kind of backing digital cash must have. For instance, must digital cash be backed by currency 100 percent? This would involve an issuer's holding $1 in currency in its vaults for every $1 of digital cash created. Alternatively, should the issuer buy short-term securities, such as U.S. Treasury bills, as backing for the digital cash? Under this system, the creation of digital cash could represent an increase in the money supply Beyond this issue lies the possibility for "designer digital cash," which could be backed by gold or issued in foreign currencies or which could earn interest. There are few technological limitations on the backing and characteristics of digital cash.

Should digital cash be covered by deposit insurance? This question needs to be settled in part to determine who is liable in the event of the failure of an issuer of digital cash. The Federal Deposit Insurance Corporation (FDIC) recently issued a notice and request for public comment addressing stored-value cards and other electronic payment systems and their eligibility for deposit insurance.11

The proposed Internet payment systems require areas of expertise new to most banks. Such expertise is typically found in software companies. Banks and bank holding companies are allowed to engage only in activities that are "closely related" to banking. It is clear from our discussion that encryption systems, among other things, are vital to the success of Internet payment systems. But is developing an encryption system an activity "closely related" to banking? By approving the acquisition of a home-banking software company by a group of U.S. and Canadian banks, and by approving the acquisition of an Internet banking software company by a subsidiary of a bank holding company, the Federal Reserve System and the Office of the Comptroller of the Currency have shown a willingness to allow banks to provide services in this area.12

Encryption systems raise issues that go beyond banking. There is a tension between the security of financial messages traveling the Internet (by means of strong encryption systems) and the security of the nation and the ability of its law enforcement authorities to prevent illegal financial transactions. The United States closely regulates the use of strong levels of encryption because of its important role in national security Some commentators fear that denial of licenses to export software that includes strong levels of encryption may put U.S. firms at a competitive disadvantage. At least one firm, though, has won approval to export software based on strong levels of encryption; its software was for financial use only, and it was felt that the encryption system could not be removed from the software.13

The need for confidentiality of payment information on the Internet is great because of the greater ease of compiling histories of consumers' purchases. Enhancements to consumer privacy laws may be needed to preclude the misuse of consumer information by nonfinancial firms that may offer payment services or affiliated software. The question of how much confidentiality is needed in Internet commerce has spawned a debate about the merits of a completely anonymous payment system versus the merits of

lower cost, more conventional systems of credit card and electronic checks that allow merchants, banks, and system operators to maintain data bases of user information.

CONCLUSION

Efforts to create a form of Internet money are attempts to put old wine in new bottles. Money must be easily identifiable, easy to protect from theft, widely acceptable, and easy to transfer. Providers of Internet payment systems are attempting to meet these requirements in various ways. Sophisticated methods of encrypting the financial information used in payments may prove to be the modern equivalent of vaults, signatures, and watermarks. Public policy will play a role in securing the legal foundations that can help pave the way to widely acceptable and secure ways to pay on the Internet.

Footnote:

IThe first of the two estimates was made by network analyst Mark Lottor, and the second refers to message traffic across the NSFNET backbone that part of the transmission lines funded by the National Science Foundation. These estimates are reported by the Merit Network, Inc., a nonprofit corporation providing a number of Internet services.

Footnote:

2The World Wide Web is a communications protocol developed for graphical content and sound.

Footnote:

3A good discussion of the Internet is given by Jeffrey K. MacKie-Mason and Hal Varian in "Economic FAQs About the Internet," Journal of Economic Perspectives, Volume 8, Number 3, Summer 1994, pp. 75-96.
Footnote:

4A killer app is an application of a particular technology that many potential users find irresistible.

Footnote:

sA good discussion of public key cryptography is contained in Bruce Schneier's book Applied Cryptography, John Wiley and Sons, Inc., second edition, 1996.

Footnote:

6An extensive list of such approaches is maintained by Michael Pierce on the Internet; the address is http://
ganges.cs.tcd.ie/mepierce/Project/oninterest.html. There are links at this site to many firms offering some of the services described in this article; those sites typically provide descriptions of the services and plans of the firms.

Footnote:
7See "Banks Get the Green Light to Hit the Internet," Bank Network News, July 12,1995.

Footnote:

sIf the merchant were to find that the cash had previously been spent, it would seem to have no recourse, given the cloak of buyer anonymity. However, David Chaum, an expert in cryptography, ingeniously devised a system in which the buyer's identity is revealed only if the buyer attempts to spend the cash twice.

Footnote:

9See the proposed rule of the Federal Reserve System, 12 CFR Part 205, Regulation E; Docket No. R-0919, April 3, 1996.

Footnote:

Il OSuch a repudiation may be done fraudulently; that is, a consumer may make a purchase using a payment system based on digital signatures and then later fraudulently claim not to have made the purchase. Hence, the effort to make it difficult to repudiate one's digital signature will reduce fraud of this sort. (Alternatively, the consumer may have mismanaged his or her private key, thereby allowing someone else to make a purchase using his or her digital signature, and repudiated the transaction for that reason.)

Footnote:

"See the notice of the FDIC in the Federal Register, August 2, 1996, pp. 40494-97.

12See the orders of the Board of Governors of the Federal Reserve System in the Federal Reserve Bulletin, April 1996, pp. 363-65, and in the issue of July 1996, pp. 674-76.

Footnote:

is..Cybercash Gets Clearance to Sell Product Abroad," Wall Street Journal, May 8, 1995.

Author Affiliation:

*James McAndrews is a senior economist and research advisor in the Banking and Financial Markets section of the Philadelphia Fed's Research Department.

?

? t1/4/

1/4/1

FN- DIALOG(R)File 347:JAPIO|
CZ- (c) 2005 JPO & JAPIO. All rts. reserv.|
TI- METHOD FOR NONBANK ELECTRONIC SETTLEMENT
PN- 10-207960 - **JP 10207960** A-
PD- August 07, 1998 (19980807)
AU- MORIMURA ICHIRO
PA- MORIMURA ICHIRO [000000] (An Individual), JP (Japan)
AN- 09-048373 -JP 9748373-
AN- 09-048373 -JP 9748373-
AD- January 27, 1997 (19970127)
IC- -6- G06F-017/60; G06F-019/00; G07D-009/00
CL- 45.4 (INFORMATION PROCESSING -- Computer Applications); 29.4 (PRECISION INSTRUMENTS -- Business Machines)
KW- R087 (PRECISION MACHINES -- Automatic Banking); R303
AB- PROBLEM TO BE SOLVED: To enable each of banking organs in various conditions to join in an electronic settlement system by only cooperating with a non-bank enterprise in status quo by making the non-bank enterprise accommodate depositors of cooperated banking organs such as city banks, local banks, credit unions, and postal savings as members and accommodate their various offices as affiliated stores.

SOLUTION: First, a member 2 uses an ATM, a bank cash card 6, and a password number to preliminarily transfer an arbitrary amount of money from the fund in his deposit account 5 of his bank 1 to his member account 7 in a non-bank enterprise 3 and applies it electronic settlement. With respect to the price to be paid to an affiliated store by the member 2, demand data, a member's card 9, the password number, and other required items are inputted to a simple transfer device 8 and are transmitted to a transfer processing center 10 of the non-bank enterprise 3 through a communication line. This center immediately collates this reception data with the balance in the member account 5; and if settlement is possible, the amount of money demanded is immediately transferred from the member account 7 to an affiliated store account 11 to terminate the electronic settlement. Required items are printed out by the simple transfer device 8.

?